Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

GIOVANI E MEDIA
PIATTAFORMA NAZIONALE PER LA PROMOZIONE DELLE COMPETENZE MEDIALI

La protezione dei dati

Dossier informativo

In collaborazione con l'Incaricato federale della protezione dei dati e della trasparenza IFPDT e la piattaforma nazionale per la promozione delle competenze mediali „Giovani e media" dell'Ufficio federale delle assicurazioni sociali UFA.

Sommario

1. Che cos'è la protezione dei dati?

Nella vita quotidiana vengono scambiate molte informazioni personali e non solo all'interno della famiglia o fra amici. Capita, ad esempio, quando si discutono i compiti a casa nella chat di classe su WhatsApp oppure si posta un nuovo selfie su Instagram, quando si è malati e lo si comunica al proprio insegnante per e-mail o SMS, quando si ordina in un uno shop online un paio di nuove scarpe sportive o in strada ci viene chiesto di partecipare a un concorso per quale è necessario indicare età e indirizzo. Per questo bisogna essere sempre consapevoli del fatto che tali dati possono anche finire nelle mani di estranei e non essere utilizzati sempre come vorremmo.

1.1. Definizione

Il termine protezione dei dati è nato nella seconda metà del 20° secolo ed è definito come protezione della sfera privata durante il trattamento dei dati e protezione del diritto all'autodeterminazione informativa. Ciò significa che ogni persona può decidere liberamente per sé quali dati personali rendere disponibili e a chi, nonché per quale scopo essi possono essere utilizzati.

Per dati personali si intendono tutte le informazioni che possono essere attribuite a una persona, quindi ad esempio:

- indirizzo
- età
- interessi e inclinazioni personali
- posizione registrata dal cellulare tramite GPS
- la sua immagine (p.es foto profilo)
- ecc.

Protezione dei dati significa che viene protetta la sfera privata delle persone i cui dati vengono trattati da autorità, aziende o privati.

In una società sempre più digitalizzata e interconnessa, la protezione dei dati ha un'importanza sempre maggiore. Essa ha lo scopo di impedire la raccolta incontrollata e l'uso abusivo di dati, la tendenza alla sorveglianza di massa, la nascita di monopoli dei dati da parte di aziende private e un eccesso di misure di sorveglianza da parte dello stato.

(Fonte: Wikipedia, traduzione dello sito tedesco)

Protezione della persona

Il termine protezione dei dati può suonare piuttosto freddo e impersonale. In realtà però, si tratta di noi stessi, cioè della protezione della nostra personalità e dei suoi diritti di base. Perché non tutte le informazioni su di noi e sulla nostra vita riguardano chiunque.

Tutti i dati che hanno qualcosa a che fare con noi sono «dati riferiti alla persona» o «dati personali». Tali dati rivelano molto di noi e sono quindi preziosi. Per le aziende essi sono come denaro contante e possono essere oggetto di abusi da parte di terzi. Ecco perché dobbiamo gestire i nostri dati personali con la massima diligenza, cioè in modo parsimonioso e ponderato. Dobbiamo essere consapevoli del valore dei nostri dati. Proteggere i nostri dati

significa proteggere la nostra **sfera privata**, l'**anonimato** e quindi godere di una **maggiore sicurezza**.

Dati degni di particolare protezione

Determinati dati personali sono considerati degni di particolare protezione perché il fatto che tali informazioni finiscano nelle mani sbagliate può avere conseguenze molto negative per le persone coinvolte. Tra i dati degni di particolare protezione vi sono tra l'altro quelli concernenti le opinioni della persona in campo religioso, ideologico e politico, ma anche le informazioni sulla salute, la sfera intima (ad es. la sessualità) o i procedimenti e le sanzioni penali.

Un elenco completo è disponibile al paragrafo «*1.1.1 Fondamenti legislativi*».

Approfondimenti

L'odierna tecnologia consente di rilevare, raggruppare e rendere disponibili le informazioni in modo praticamente illimitato. Per questo il rischio potenziale di violazioni della personalità è aumentato. Il singolo individuo non è infatti più in grado di controllare quali dati personali vengono trattati e da chi. Quotidianamente comunichiamo, volontariamente o involontariamente, dati su di noi a persone terze, senza sapere per quali scopi esattamente verranno utilizzati e per quanto tempo resteranno archiviati. Oggi le aziende possono, ad esempio, scoprire se un cliente è un buon o un cattivo pagatore, quali libri legge o quale musica ascolta senza che la persona in questione ne sia consapevole.

Quando vengono raccolte e trattate informazioni su persone, ciò ha un impatto sulla loro personalità. Tale impatto può essere più forte o più debole e causare reazioni positive o negative. Una persona può restare «macchiata» per tutta la vita se dati negativi che la riguardano vengono conservati a tempo indeterminato e continuamente riutilizzati. Per questo i dati personali sono un bene da proteggere. Per la persona stessa, ma anche per persone terze che abbiano un interesse in tal senso.

Obiettivo della protezione dei dati è appunto proteggere questo bene prezioso. La protezione dei dati fissa dei paletti per il trattamento dei dati personali, al fine di garantire che lo sviluppo della personalità non venga compromesso dal trattamento indesiderato di dati. Laddove l'ordinamento giuridico non preveda altrimenti, chiunque deve poter decidere in merito alla comunicazione e all'utilizzo dei propri dati personali. *(cfr. il messaggio concernente la Legge federale sulla protezione dei dati, LPD 23 marzo 1998, cifra 113: Obiettivi generali di una legge sulla protezione dei dati)*

Ciascuno ha inoltre il diritto di sapere chi è in possesso di informazioni sul suo conto, quali sono tali informazioni e per quali scopi vengono utilizzati i relativi dati. Abbiamo anche il diritto di chiedere al titolare di una raccolta di dati di comunicarci i nostri dati personali in suo possesso, nonché di farli correggere o cancellare.

Perché la protezione dei dati è importante

La **tecnologia dell'informazione** consente di **rilevare e mettere in relazione tra loro enormi quantitativi di dati personali** (parole chiave: Big Data, intelligenza artificiale, Internet of Things). Spesso la consapevolezza in materia di sicurezza di chi tratta i dati non tiene il passo delle novità tecnologiche. Inoltre, la maggior parte delle persone – siano esse dal lato di chi tratta i dati o persone i cui dati vengono trattati – non sono ancora sufficientemente sensibilizzate sul tema della protezione della personalità.

Molte persone gestiscono i propri dati personali in modo molto superficiale, sia su Internet che compilando **moduli per sondaggi o concorsi** o ancora **utilizzando diverse app sul proprio smartphone** (attivazione della localizzazione, comunicazione di informazioni personali sui social network ecc.), per citare solo alcuni esempi.

Non solo a causa delle crescenti possibilità offerte dalla tecnologia e dei rischi ad esse correlati (perdita di dati, furto di identità ecc.) sono necessari paletti per proteggere la sfera privata. La protezione dei dati è un requisito fondamentale anche per l'esercizio delle libertà come la libertà di opinione, la libertà di credenza e la libertà di riunione.

Infatti, esprimereste ancora liberamente il vostro parere se doveste temere di essere intercettati? Come votereste se doveste farlo pubblicamente e indicando il vostro nome?

L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) garantisce che i paletti fissati nella legge sulla protezione dei dati siano rispettati. Inoltre, fornisce consulenza a privati e organi federali per quanto concerne il rispetto delle disposizioni di legge in materia di protezione dei dati. L'IFPDT deve quindi informare e sensibilizzare, ma anche intervenire se i titolari di raccolte di dati non rispettano i principi della protezione dei dati.

(vedi anche https://www.edoeb.admin.ch/edoeb/it/home/l-ifpdt/mandato.html)

1.1.1. Fondamenti legislativi

Convenzione europea dei diritti dell'uomo (CEDU)

Art. 8 Diritto al rispetto della vita privata e familiare

[1] Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

[2] Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

La protezione dei dati nella Costituzione federale:

Art. 13 Protezione della sfera privata

[1] Ognuno ha diritto al rispetto della sua vita privata e familiare, della sua abitazione, della sua corrispondenza epistolare nonché delle sue relazioni via posta e telecomunicazioni.

[2] Ognuno ha diritto di essere protetto da un impiego abusivo dei suoi dati personali.

Scopo della protezione dei dati è quindi proteggere le informazioni relative alle singole persone. Ognuno ha il diritto di determinare autonomamente quali informazioni che lo riguardano devono essere rese note quando, dove e a chi. La protezione dei dati fa in modo che vengano sempre raccolti e trattati tutti i dati necessari ma il minor quantitativo di dati possibile. Ogni persona ha inoltre il diritto di prendere visione dei dati sul suo conto che vengono registrati!

Codice civile svizzero (CCS)

Art. 281B. Protezione della personalità / II. Contro lesioni illecite / 1. Principio

II. Contro lesioni illecite

1. Principio

[1] Chi è illecitamente leso nella sua personalità può, a sua tutela, chiedere l'intervento del giudice contro chiunque partecipi all'offesa.

[2] La lesione è illecita quando non è giustificata dal consenso della persona lesa, da un interesse preponderante pubblico o privato, oppure dalla legge.

Vedi inoltre: Art. 28a segg. CCS (Protezione della personalità).
https://www.admin.ch/opc/it/classified-compilation/19070042/index.html#a28a

Legge federale sulla protezione dei dati (LPD):

Art. 1 Scopo

Scopo della presente legge è di proteggere la personalità e i diritti fondamentali delle persone i cui dati sono oggetto di trattamento.

(…)

Art. 4 Principi

[1] I dati personali possono essere **trattati soltanto in modo lecito**.

[2] Il trattamento dei dati deve essere **conforme al principio della buona fede** e della proporzionalità.

[3] I dati possono essere trattati **soltanto per lo scopo** indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge.

[4] La raccolta di dati personali e in particolare le finalità del trattamento devono essere **riconoscibili** da parte della persona interessata.

[5] Quando il trattamento di dati personali è subordinato al consenso della persona interessata, il consenso è valido soltanto se espresso **liberamente e dopo debita informazione**. Trattandosi di dati personali degni di particolare protezione o di profili della personalità, il consenso deve essere anche esplicito.

Dati personali degni di particolare protezione nella Legge federale sulla protezione dei dati

Art. 3 Definizioni

c. dati personali degni di particolare protezione:
i dati concernenti:
1. le opinioni o attività religiose, filosofiche, politiche o sindacali,
2. la salute, la sfera intima o l'appartenenza a una razza,
3. le misure d'assistenza sociale,
4. i procedimenti o le sanzioni amministrativi e penali.

Modifiche previste nella nuova legge sulla protezione dei dati

Nella nuova Legge federale sulla protezione dei dati (LPD) è previsto che, oltre a quelli già elencati, anche i dati biometrici e genetici, nonché i profili della personalità siano considerati dati personali degni di particolare protezione.

1.1.2. Conclusioni

Considerando i progressi tecnologici sopraccitati e le possibilità che offrono di salvare e mettere in relazione più velocemente grandi quantitativi di dati personali, confrontarsi con la questione della protezione dei dati è indispensabile.

Proprio grazie alle possibilità offerte da Internet, i dati sono rapidamente accessibili a persone terze e ciò che è una volta «online» non può più essere completamente cancellato o corretto o può esserlo solo con grande difficoltà. Internet non dimentica mai.

In quanto privati, è importante in particolare conoscere i propri diritti e sapere in che modo attivarsi qualora i propri dati personali vengano illegittimamente salvati, trattati o comunicati a terzi. Il presente dossier informativo, con le schede e i compiti ad esso correlati, ha lo scopo di fornire aiuto in tal senso.

Inoltre, è di fondamentale importanza rispettare personalmente le direttive in materia di protezione dei dati, gestendo i propri dati in modo consapevole e trattando correttamente quelli di terzi. A tale scopo nel capitolo 3 «Consigli per una corretta gestione dei dati» fornisce avvertenze e consigli concreti su come comportarsi.

1.2. Chi è interessato ai dati personali? Chi li raccoglie e perché?

Ci sono diversi motivi per i quali qualcuno può dimostrare interesse nei confronti dei nostri dati personali.

1.2.1. Raccolta di dati da parte dello stato

Soprattutto negli stati autoritari e totalitari, le autorità statali hanno interesse a sapere come si comportano i propri cittadini. In questi casi l'obiettivo è ottenere il controllo sui cittadini (parola chiave: «cittadino trasparente»).
Un esempio particolarmente grave è stata la sorveglianza sociale praticata nella Germania nazionalsocialista tra il 1933 e il 1945, dove vennero stilate liste dei nemici politici in generale e degli ebrei in particolare. Oltre a garantire il potere dei nazionalsocialisti, l'obiettivo era l'annientamento totale degli ebrei. La stella di David – gli ebrei dovevano mostrare in qualsiasi momento la propria appartenenza alla religione ebraica portando la stella cucita sugli abiti – era una violazione particolarmente «appariscente» dell'attuale concezione di protezione dei dati.

Tuttavia, anche in nazioni democratiche come la Svizzera vengono raccolti dati e osservati e sorvegliati individui. Nei tardi anni '80 venne alla luce che le autorità federali svizzere e le autorità di polizia cantonali avevano creato circa 700'000 schede di archivio, raccogliendo così dati sensibili e informazioni di carattere ideologico su oltre il 10% dei cittadini svizzeri. Ufficialmente l'obiettivo era proteggere il paese dal «rischio del comunismo». La conseguenza del cosiddetto «scandalo delle schedature» fu che la fiducia dei cittadini nello stato fu scossa per molto tempo.
Anche oggi però le autorità raccolgono dati, in modo ufficiale e legale. Ad esempio in Svizzera vengono tenuti sotto sorveglianza i membri di gruppi estremisti o criminali oppure le persone che hanno relazioni con il terrorismo internazionale. Tale compito è svolto dal

Servizio delle attività informative della Confederazione (SIC), che è assoggettato al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS).
Ovviamente, in uno stato di diritto non è consentito sorvegliare qualcuno senza motivo. Esistono severi fondamenti giuridici che regolano una tale intromissione nei diritti personali. Le azioni dello stato devono pertanto essere **previste da una legge** (ad es. codice di procedura penale, Legge federale sulle attività informative). Si parla del principio di **legittimità**).
Per le inchieste, le indagini e la sorveglianza di persone vale inoltre il principio della **proporzionalità**. È necessario valutare sempre se l'intromissione in interessi privati e diritti fondamentali sia o meno giustificata dall'interesse pubblico generale.

Legittimità e proporzionalità nella Costituzione federale (CF):

Art. 5 Stato di diritto

[1] *Il diritto è fondamento e limite dell'attività dello Stato.*

[2] *L'attività dello Stato deve rispondere al pubblico interesse ed essere proporzionata allo scopo.*

1.2.2. Raccolta di dati di privati e aziende

Provider Internet e servizi online

Chi utilizza servizi via Internet con il computer, il tablet o il telefono cellulare, genera automaticamente dei dati. Tali dati possono essere archiviati da parte dei provider Internet. In tal modo è possibile stabilire su quali siti Internet naviga una persona e per quanto tempo oppure quale app utilizza. Per le aziende tali dati sono interessanti e significativi poiché, tra l'altro, forniscono informazioni sui consumi e le preferenze degli utenti di Internet. Ciò permette ad es. anche di visualizzare all'utente pubblicità personalizzata, tagliata su misura per i suoi interessi. A chi visita spesso portali di shopping online o utilizza app per lo shopping, può quindi capitare di trovare nel proprio browser o direttamente nella app proposte di altri articoli o servizi che potrebbero piacergli.

Assicurazioni

Sulla base di statistiche, che di norma vengono pubblicate con dati resi anonimi, è possibile definire gruppi di rischio e di conseguenza pretendere premi assicurativi più elevati per singoli gruppi. Ciò è possibile, ad esempio, nel caso delle statistiche sugli incidenti stradali: in base all'età e al sesso determinate categorie di assicurati pagano premi più elevati di altri perché il loro «gruppo» causa statisticamente più incidenti. In compenso pagano meno per la cassa pensioni perché di norma si ammalano meno.

Tuttavia, per la definizione di modelli assicurativi tagliati su misura o per la partecipazione a programmi di bonus, le compagnie di assicurazioni raccolgono sempre più spesso informazioni personali, tra cui anche dati degni di particolare protezione sulla salute o sui profili di movimento.

Commercianti al dettaglio

I profili dei clienti aiutano i commercianti al dettaglio ad analizzare il comportamento dei loro clienti come consumatori. In tal modo possono orientare la loro offerta di merce e la pubblicità realizzando più fatturato e più utili. L'acquirente rischia però di essere indirettamente manipolato.

Moduli per sondaggi e concorsi

In genere questi moduli costituiscono la base mediante la quale le aziende personalizzano la propria pubblicità, potendola così indirizzare a clienti potenziali.

Gli indirizzi e gli altri dati personali sono di grande importanza per il marketing diretto. Con l'ausilio di informazioni il più possibile precise su età, professione, comportamento relativo agli acquisti ecc. è possibile ridurre il rischio di effettuare pubblicità inutile. Tra la popolazione esiste una notevole disponibilità a fornire informazioni. Vengono comunicati perfino dati intimi, se gli intervistati sono convinti che i loro dati servano per un progetto scientifico. Particolarmente fruttuoso sembra essere lo svolgimento di sondaggi di questo tipo in combinazione con la partecipazione a un concorso o a un gioco a premi nel quale la rilevazione dei dati sia uno scopo non chiaramente individuabile. In genere, l'indicazione che i dati possono essere utilizzati per altri scopi è contenuta nelle avvertenze in carattere piccolo alle quali spesso non si fa caso. In tal modo i potenziali clienti vengono indotti a comunicare i propri dati. Tali raccolte di dati mascherate a scopo commerciale non sono lecite.

Agenzie d'informazioni creditizie, economiche e commerciali

Le agenzie d'informazioni raccolgono informazioni su persone che non pagano puntualmente una fattura oppure ricevono un'ingiunzione di pagamento o un'esecuzione, classificandole come insolventi anche se a volte il tutto si rivela essere solo un malinteso. In tal caso può accadere che a una persona venga ad esempio negata la stipulazione di un contratto di telefonia mobile o che un'azienda di vendite per corrispondenza sia disposta a consegnare solo contrassegno.

Altri soggetti che possiedono informazioni sulle abitudini di pagamento sono i cosiddetti servizi di incasso. Si tratta di aziende private che provvedono a riscuotere le fatture in sospeso. Spesso i servizi di informazione e di incasso vengono offerti dalla stessa azienda.

I dati contenuti in queste raccolte comprendono, oltre ai dati del debitore, anche quelli concernenti il tipo di debito, la data a cui risale e l'importo. I dati provengono da diverse fonti che possono, ad esempio, essere accessibili al pubblico via Internet. Prima di stipulare un contratto, gli interessati possono chiedere all'agenzia se la futura controparte è degna di fiducia e se onora gli impegni finanziari.

Se i dati sono errati, la persona in questione ne può pretendere la cancellazione o la correzione.

2. Le moderne tecnologie informatiche e i loro rischi

2.1. Internet e computer

2.1.1. Web 2.0 – un'idea con tanti trabocchetti

Da alcuni anni, le persone che navigano su Internet non sono più solo «consumatori», bensì utilizzano Internet sempre più spesso per diffondere informazioni, foto, video ecc. I siti Internet diventano più dinamici e interattivi. Nel gergo informatico questa evoluzione è detta **Web 2.0**.

Sempre più importanti diventano inoltre le cosiddette «reti sociali» o, in inglese, «Social Networking Sites» (SNS o più comunemente «social network»).

In genere gli utenti di questi portali Internet creano un profilo contenente indirizzi, preferenze, foto e altri dati e informazioni. In base alle impostazioni scelte, tale profilo può essere accessibile a tutti gli utenti di Internet. Di norma le impostazioni standard sono configurate in modo che l'utente fornisca automaticamente più dati su di sé del necessario, a meno che le impostazioni non vengano modificate dopo la registrazione. Per questo è opportuno verificare le impostazioni relative alla privacy di ogni servizio e modificarle secondo le preferenze individuali. Bisogna assegnare i diritti in modo che solo un determinato gruppo di persone abbia accesso al profilo. Spesso invece, con le impostazioni standard, si comunicano moltissime informazioni personali senza esserne consapevoli.

Il fatto che gli utenti di Internet pubblichino molte informazioni su se stessi e volontariamente, pone la protezione dei dati davanti a nuove problematiche. Se mettiamo in rete informazioni su altre persone senza che ci sia richiesto, violiamo la loro sfera privata e le disposizioni della legge sulla protezione dei dati.

Dal punto di vista della protezione dei dati vanno considerati i seguenti punti:

- Gli utenti dei social network presentano volontariamente a un vasto pubblico numerosi dati prima considerati personali o privati.
- In tal modo privati, aziende, uffici governativi ecc. ottengono un accesso semplice e anonimo a dati personali.
- Gli utenti dei social network possono caricare anche dati di persone non iscritte, rendendoli così ugualmente accessibili al pubblico per un'ulteriore diffusione.

Ne risultano diversi **rischi** cui si espone un utente di queste piattaforme:

- **Internet non dimentica.** I profili degli utenti possono essere scaricati e salvati da altri utenti, il che rende la cancellazione del profilo originario quasi inutile poiché i dati vengono comunque mantenuti. In tal modo si genera un enorme numero di raccolte di dati private e cresce il rischio che tali dati vengano utilizzati in modo differente da quello originariamente previsto.
- I provider di SNS hanno accesso non solo ai dati personali, ma anche ai cosiddetti dati marginali come: ora del login e durata della connessione, origine geografica dell'indirizzo IP, permanenza, movimenti sul sito ecc.
- Nel caso di molti provider di SNS non è chiaro come vengano utilizzati tali dati. Chiaro è invece che, sulla base dei dati personali e di quelli aggiuntivi, è possibile creare

profili dettagliati della personalità la cui vendita frutta notevoli guadagni e il cui utilizzo può risultare svantaggioso per le persone interessate.

- **Riconoscimento automatico del volto:** su Facebook, Instagram, Google+ e piattaforme simili, gli utenti possono marcare (taggare) amici e conoscenti sulle foto. Grazie al riconoscimento automatico del volto, il sistema scansiona ogni nuova immagine per individuare amici di un utente già noti e taggati, proponendone il nome. A quel punto è sufficiente un clic e, da quel momento in poi, l'amico sarà marcato con l'indicazione del nome in tutte le foto nelle quali è raffigurato. Su alcune piattaforme questa funzionalità è attivata automaticamente e chi non desidera essere taggato deve procedere alla sua disattivazione nelle impostazioni relative alla privacy.
- In una direzione simile va anche il rischio di **riconoscimento** automatico di caratteristiche nello sfondo di un'immagine. Per geolocalizzare una foto possono essere utilizzati ad es. paesaggi o case presenti sullo sfondo. Ancor più facilmente una foto può essere attribuita a un luogo e a un determinato momento sulla base dei metadati salvati. I metadati sono informazioni aggiuntive salvate in un file di immagine come ad es. informazioni sul luogo in cui è stata scattata la foto, la data e l'ora.
- Alcune piattaforme consentono anche di caricare dati di persone terze che non sono iscritte al social network, il tutto senza chiederne il consenso. Ciò può comportare rischi per la sfera privata delle persone coinvolte o quantomeno non essere nel loro interesse.
- In pratica gli account utente non possono mai essere cancellati in modo definitivo. Da un lato i profili vengono in parte solo disattivati e non cancellati. Dall'altro lato gli utenti attivi lasciano ulteriori informazioni in altre pagine del social network. Cancellarle tutte risulta praticamente impossibile. In tal modo gli utenti perdono il controllo dei propri dati.
- Nella maggior parte dei social network, gli ostacoli da superare per la registrazione sono molto bassi: basta inserire alcuni dati personali che non vengono verificati e possono quindi essere anche inventati. Ciò è positivo dal punto di vista della protezione dei dati, perché la persona può evitare di essere riconosciuta, ma comporta anche dei rischi per coloro che entrano in contatto con tali utenti «inventati». Una volta iscritti, può risultare molto semplice stringere contatti ed essere accolti nelle cerchie di amici di altri. Se persone con cattive intenzioni fingono di essere amiche per ottenere informazioni, può crearsi una situazione rischiosa.

Il tipico utente di Android (in inglese):
http://allthingsd.com/20111229/if-android-were-a-single-person-heres-what-he-would-look-like/

2.1.2. Raccolte di dati in formato digitale

Attraverso i moduli per la partecipazione a sondaggi e concorsi, ma soprattutto tramite il «Web 2.0» i suoi innumerevoli social network e piattaforme di comunicazione, finiscono in circolazione enormi quantitativi di dati. Con le odierne tecnologie informatiche è facilissimo rilevare dati personali, salvarli, analizzarli, organizzarli e utilizzarli per agire. Nella «web-community», cioè la comunità di Internet, nessuno può evitare che i suoi dati lascino tracce in qualche luogo e vengano utilizzati per scopi diversi.

Anche in questo caso le aziende sono interessate alle entrate derivanti dalla pubblicità effettuata mediante offerte adeguate all'utente. I seguenti capitoli sono dedicati ai rischi delle moderne tecnologie digitali.

2.1.3. Trasmissione di dati mediante supporti digitali

I supporti dati mobili e in particolare le chiavette USB comportano rischi che vengono spesso sottovalutati. Essi possono infatti trasmettere virus e, in caso di smarrimento, mettere a rischio la sicurezza dei dati personali. Seguendo alcune regole, tali rischi possono essere fortemente ridotti.

Secondo quanto riportato dai media, negli ultimi mesi numerose organizzazioni sono state infettate con programmi dannosi mediante supporti dati. Secondo uno studio americano, la quota di virus trasmessi mediante chiavette USB negli ultimi anni è notevolmente aumentata. Per trasmettere virus è sufficiente collegare il supporto dati al computer e il «malware» può installarsi sul disco rigido.

LanLine: la chiavetta USB, un punto debole sottovalutato (in tedesco)
http://www.lanline.de/unterschaetzte-schwachstelle-usb-stick/

In realtà è possibile proteggere i propri dati in modo relativamente semplice dagli attacchi provenienti da chiavette USB.

- La funzione Autorun per le chiavette USB deve essere disabilitata sul computer al fine di impedire che dati vengano trasferiti automaticamente. Si tratta di un'impostazione che è possibile effettuare con pochi clic tramite l'interfaccia del sistema operativo. Sotto «Avvio automatico» è possibile spuntare la voce «No» per evitare che il computer avvii una chiavetta USB senza prima chiedere.
- Inoltre, è consigliabile effettuare la scansione antivirus della chiavetta come si fa per il disco rigido. A tale scopo va utilizzato un antivirus che analizzi i file presenti sulla chiavetta e, se necessario, li disinfetti.
- Affinché i dati personali non finiscano nelle mani sbagliate in caso di smarrimento di un supporto digitale è opportuno criptarli.

Chip.de: UsbFix2017 (scansione antivirus per chiavette USB e dischi rigidi) (in tedesco)
http://www.chip.de/downloads/UsbFix-2017_74217923.html

Selbstdatenschutz.info: criptare il disco rigido esterno o la chiavetta USB con Windows (in tedesco)
https://www.selbstdatenschutz.info/windows/externe_datentraeger_verschluesseln/

2.1.4. La marea di dati digitali comporta dei rischi

Negli ultimi due decenni la nostra vita è stata profondamente modificata e, nei casi positivi, semplificata dall'avvento del World Wide Web e dei servizi ad esso correlati. Possiamo infatti comunicare senza problemi e in tempo reale in tutto il globo. La quantità e gli scambi di dati che si generano causano però anche dei pericoli per gli utenti. Le informazioni personali, i testi, i video e le foto che vengono caricati in rete, a partire da quel momento non sono più privati. Una volta in rete i dati sviluppano una vita propria. Si diffondono, finiscono in motori di ricerca e archivi online (ad es. thearchive.org) e vengono copiati o inoltrati da altri utenti. Annullare e cancellare tutto è quasi impossibile.

Il World Wide Web non dimentica (quasi) nulla!

La moltitudine di dati viene trasmessa automaticamente senza che ce ne accorgiamo.

Tutte le volte che navighiamo su Internet (sia dal PC di casa che con lo smartphone) l'accesso viene registrato mediante un cosiddetto indirizzo IP (una specie di «numero di telefono» su Internet). In tal modo è possibile ricostruire con precisione quando un utente naviga utilizzando quel numero, per quanto tempo e quali pagine visita. L'indirizzo IP viene riassegnato a ogni accesso a Internet, ma il provider Internet protocolla tutti gli accessi effettuati con i diversi indirizzi IP. Il provider può quindi ricostruire in qualsiasi momento con quale numero è avvenuta la navigazione, per quanto tempo, con quale frequenza e quali pagine sono state visitate.

Mediante l'indirizzo IP la polizia può indagare su reati, come ad esempio gli upload illegali di musica, risalendo agli autori. Anche le aziende registrano gli indirizzi IP riuscendo così, in alcune circostanze, a stabilire se un computer ha già effettuato un accesso al sito Web oppure no. Quindi, navigando in Internet, si lascia un'**impronta digitale** che fornisce informazioni sul nostro modo di navigare. Inoltre, la navigazione lascia tracce anche sul nostro computer o smartphone.

2.2. Webtracking

2.2.1. Cookie

Con l'ausilio dei cosiddetti «**Cookie**» (*inglese: biscotti*) vengono creati profili di dati. I profili contengono ad esempio informazioni sulle nostre preferenze durante la navigazione, i banner pubblicitari sui quali abbiamo cliccato e il tempo di permanenza sui rispettivi siti Web. Il cookie in sé è un piccolo file che il server salva sul proprio disco rigido quando vengono letti determinati file Internet. Può essere una funzionalità pratica perché fa sì che, navigando e visitando siti Web, non sia necessario ripetere continuamente le stesse impostazioni (ad es. la scelta della lingua), ma vengono utilizzati anche per altri scopi. Non è possibile escludere conseguenze poco piacevoli. Dato che i cookie vengono salvati in modo invisibile, l'utente nella maggior parte dei casi non sa che cosa contengono e determinano: in molti casi ciò significa una marea di pubblicità indesiderata orientata secondo il comportamento e il gruppo di destinatari.

2.2.2. Integrazione di social plugin

Integrando social plugin i gestori di siti Internet possono utilizzare determinati servizi di reti sociali sulle proprie pagine web. Il tasto «Mi piace» di Facebook, per esempio, consente ai visitatori di un sito di condividere con un clic una pagina web sul loro profilo Facebook. I gestori di siti Internet puntano così a una rapida diffusione della loro pagina. Il collegamento è inoltre utilizzato per ottenere dati statistici dettagliati sui loro utenti. I social plugin producono una trasmissione automatica di dati all'offerente interessato. In Facebook, per esempio, già al momento dell'accesso vengono trasmessi dati quali l'indirizzo IP dell'utente e l'indirizzo del sito visitato – indipendentemente dal fatto che l'utente abbia cliccato il tasto «Mi piace», abbia effettuato il login su Facebook o sia registrato in Facebook. Allo stesso tempo viene inviato – se disponibile – un cookie installato precedentemente.

Se l'utente Internet naviga e contemporaneamente ha effettuato il log-in nella rete sociale, i dati di tracking possono far risalire direttamente a lui. Se clicca sul tasto «Mi piace», a ciò si aggiunge l'informazione che gli piace un determinato contenuto. In tal modo è possibile tracciare profili d'utente dettagliati e in particolare indirizzare pubblicità personalizzata agli utenti e alla loro cerchia di amici in rete.

2.2.3. Che cosa possono fare gli utenti di Internet per evitare la tracciatura

In primo luogo è consigliabile cancellare **i cookie salvati e la cronologia del browser** dopo ogni sessione oppure impostare il browser in modo che la cancellazione avvenga automaticamente a ogni chiusura del programma.
L'utente ha inoltre la possibilità di bloccare il salvataggio di cookie di fornitori terzi nel proprio browser. Questa strategia è tuttavia inefficace contro i cosiddetti «flash cookie», che vengono salvati sul computer indipendentemente dal browser. È pertanto opportuno disattivarli nel manager delle impostazioni del Flash Player, disponibile nelle impostazioni di sistema, se tale programma è stato installato.
L'installazione di piccoli **pacchetti software («Add on»)** nel browser consente all'utente di osservare quali servizi di tracciatura lo stanno seguendo e, in base al prodotto, di bloccarli specificamente nelle impostazioni. Tuttavia anche con queste piccole applicazioni bisogna essere prudenti: programmi apparentemente utili possono contenere trojan che succhiano file. Consiglio: scaricare solo app provenienti da fonti affidabili, effettuare gli update periodici e cancellare le app non più necessarie.
Ormai molti browser dispongono della **funzione antitracciatura**, che può essere attivata nel browser e segnala che non si desidera essere tracciati («do not track»).
L'utente di Internet non vede tuttavia se la controparte si attiene a tale indicazione. Dal punto di vista della protezione dei dati, il mancato rispetto di una tale dichiarazione di dissenso costituisce un'illegittima violazione della personalità.

Cfr. IFPDT, Spiegazioni sul web tracking
https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/webtracking/spiegazioni-sul-web-tracking.html

Bluewin.ch (in tedesco) – come riconoscere i siti Web non sicuri
https://www.bluewin.ch/de/digital/redaktion/2017/17-07/so-erkennen-sie-unsichere-websites.html

2.3. Social network e chat

Esempi: Facebook, Instagram, Snapchat, Twitter, Pinterest ecc.

Chi desidera utilizzare il maggior numero possibile di funzioni dei social network, può facilmente cedere alla tentazione di rivelare molto di sé. In tal modo si corre il pericolo di diventare identificabili e ci si espone a diversi rischi, come ad esempio quello di ricevere contatti indesiderati. Ciò evidenzia la problematicità della presenza sui social network: «Per partecipare, mi devo mostrare» – una nuova forma di pressione sociale.

Ormai tutti i social network prevedono impostazioni relative alla visibilità delle informazioni mediante le quali l'utente può decidere autonomamente QUALI informazioni rendere visibili IN CHE MODO e A CHI.

Il grafico qui sotto mostra il ruolo sociale che occupano oggi i social network nel panorama di Internet.

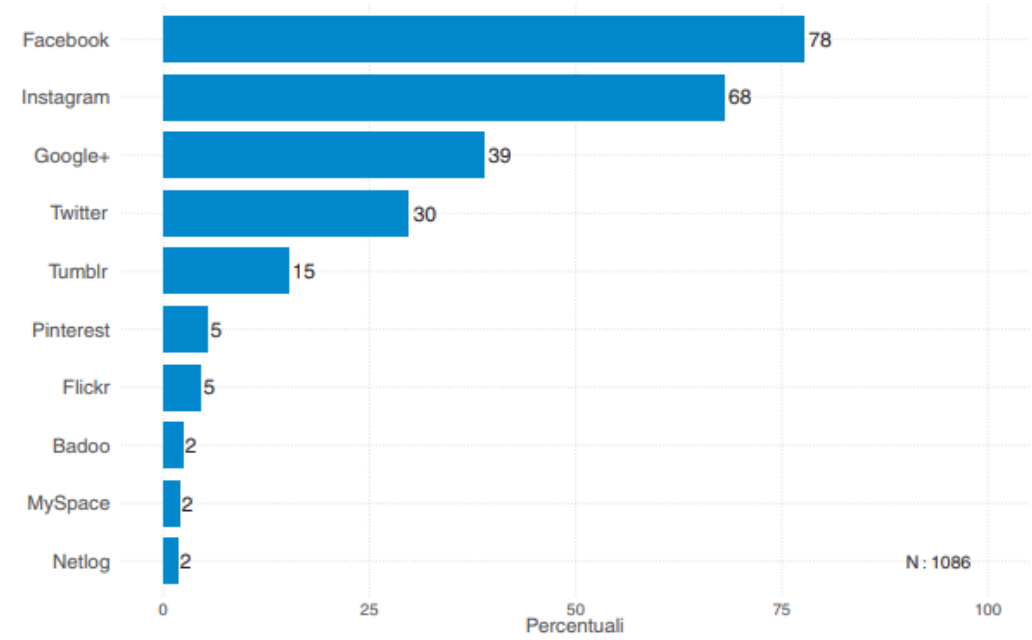

Figura 37: affiliazione a social network

(Fonte: https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2014/Rapporto_JAMES_2014.pdf)

L'aspetto problematico è che ci sono sempre network nei quali, dopo l'iscrizione, è necessario modificare attivamente le impostazioni relative alla sicurezza per la protezione della sfera privata. Sarebbe invece auspicabile che al momento dell'iscrizione fosse preimpostato il livello di sicurezza massimo e che l'utente lo potesse poi ridurre se lo desidera («Privacy by default»).

Ma cosa succede se, a causa di un'anomalia tecnica, vengono resi pubblici foto e commenti che solo pochi amici avrebbero dovuto vedere? Che ciò possa accadere, il visionario e fondatore di Facebook Mark Zuckerberg nel 2011 lo ha sperimentato sulla propria pelle: alcune sue foto personali sono state visibili a tutti per breve tempo e ora possono essere trovate in rete su altri siti.

Foto di Zuckerberg pubblicate per errore

http://www.repubblica.it/esteri/2018/03/21/news/scandalo_facegbook_parla_zuckerberg_sono_responsabile_di_quanto_successo_-191888329/

2.3.1. Quali dati raccoglie Google?

Alla fine degli anni '90 due studenti di informatica hanno fondato l'azienda «Google» che è nota in primo luogo per il suo motore di ricerca. Nel frattempo però Google offre anche numerosi altri popolari servizi online. Ecco alcuni esempi di dati che noi mettiamo, consapevolmente o inconsapevolmente, a disposizione di Google:

Ricerca su Google:
codice nazione
criteri di ricerca
indirizzo IP
lingua
numero di risultati
Safe search on/off
clic sui risultati della ricerca
cookie / tipo di browser

Youtube:
tutti i video caricati
tutti i commenti
video segnalati
canali
video visualizzati
trasferimento dati
comportamento con i clic
nazione
cookie / tipo di browser

Blogger:
foto degli utenti
data di nascita
nazione
trasferimento dati
dimensioni dei dati
clic
post

Account di Google:
data di registrazione
nome utente
password
indirizzo e-mail alternativo
nazione
numero di login
servizi Google utilizzati
cookie / tipo di browser

Per utenti registrati:
indirizzo e-mail
password
nome utente
preferiti
gruppi
contatti

Google-Docs:
indirizzo e-mail
numero di login
numero di azioni
dimensioni dei dati
clic
tutti i testi
tutte le foto
tutte le modifiche
dati di registrazione

Google Toolbar
siti Web visitati (tutti)
tutte le pagine 404

funzione di sincronizzazione con l'account di Google

Traduttore di Google
tutti i testi tradotti
cookie / tipo di browser

Google Mail
tutte le e-mail
tutte le attività dell'account
spazio in memoria
numero di login
link cliccati
liste di contatti
traffico dati
dimensioni dei dati

Conclusioni
Questi sono solo alcuni dei servizi che ci vengono offerti gratuitamente. Dobbiamo essere sempre consapevoli che questi servizi non sono mai veramente «gratis», in quanto li paghiamo con i nostri dati. È un dato di fatto che Google & Co. raccolgono moltissimi dati. In parte ciò è necessario, perché altrimenti alcuni servizi non possono funzionare. Tuttavia, chi

utilizza molti servizi può essere facilmente classificato e catalogato. Possono essere creati profili della personalità molto vasti. Tali dati vengono utilizzati primariamente per inviare pubblicità personalizzata. Il motore di ricerca di Google infatti ottimizza i risultati della ricerca in base al profilo. In tal modo chi effettua la ricerca trova più rapidamente ciò che vuole, perché viene classificato sulla base del suo profilo. La questione è se l'utente desideri effettivamente essere catalogato e ottenere una selezione di risultati generata dal computer.

2.3.2. Perché ad es. Facebook raccoglie i dati degli utenti?

Tramite la piattaforma Facebook utenti di tutto il mondo comunicano, parlando non solo dei propri hobby e della propria visione del mondo. Anzi, molti utilizzano Facebook come una specie di memoria o fotoarchivio personale al quale possono accedere ovunque si trovino. Soprattutto per persone con un elevato grado di mobilità, ciò offre la possibilità, apparentemente conveniente, di restare in contatto avendo a disposizione semplicemente una connessione a Internet. Chi desidera sapere perché Facebook raccoglie i dati degli utenti, compresi quelli cancellati, deve partire dalla storia dell'azienda e dal suo modello commerciale.

La piattaforma pubblicitaria Facebook

La maggior parte delle offerte pubblicitarie su Internet hanno lo svantaggio di essere proposte in modo quasi casuale a chiunque visualizzi in quel momento il sito Internet in questione. Per questo la maggior parte della pubblicità pubblicata su Internet sotto forma di banner o link non viene letta, in quanto troppo generica per il singolo utente. L'idea che sta dietro il cosiddetto social network Facebook è personalizzare la pubblicità. Fornendo dati relativi alla propria professione e ai propri hobby, si riceve la pubblicità corrispondente. Ciò avviene direttamente sulla pagina del proprio profilo oppure, in caso di consenso all'invio tramite altri canali, anche per e-mail o attraverso altre piattaforme di comunicazione. In tal modo gli inserzionisti evitano di pagare clic inutili. Dato che tutti gli utenti di Facebook effettuano il login con un nome che si sono scelti, l'azienda sa sempre chi è seduto davanti al computer. Sulla base di dati aggiuntivi come il luogo di domicilio, la professione e l'età è anche possibile stimare il reddito probabile. Così gli inserzionisti scoprono l'età, la classe di reddito e, in base ai dati forniti dall'utente, anche gli interessi del singolo individuo.

A ogni clic Facebook impara a conoscere meglio l'utente

Grazie ai famosi pulsanti «Mi piace», Facebook impara ogni volta qualcosa sui propri utenti, cioè su di noi e sulle nostre preferenze. Se siamo amanti dei viaggi per mare ci può venire offerta una crociera di lusso oppure una crociera per giovani. Per questo praticamente tutti i dati relativi al passato valgono come denaro contante. A ogni clic il profilo dell'utente diventa più chiaro e interessante per l'industria pubblicitaria. Questo costituisce il vero valore di Facebook. A proposito, anche semplicemente visitando un sito Web con pulsante «Mi piace» vengono forniti all'azienda dati che vengono correlati al profilo con cui è stato effettuato il login.

Troppe cancellazioni rendono Facebook senza valore

Un'indagine sulle modalità con cui Facebook applica la protezione dei dati richiesta da uno studente viennese scuote le fondamenta dell'azienda. Se le informazioni fornite fino a un determinato momento possono essere semplicemente cancellate, l'utente riottiene una parte

del controllo sul proprio profilo. Tuttavia Facebook è interessante per l'industria pubblicitaria solo se sono disponibili informazioni complete. Ora l'azienda stessa ha rivelato che non viene dato seguito alla richiesta dell'utente di cancellare i dati. I dati infatti non vengono cancellati presso il centro di calcolo, bensì semplicemente disattivati, cioè impostati su uno stato che li rende «invisibili».

Che cosa può fare l'utente di Facebook contro questa situazione?
La raccomandazione concreta è di considerare la questione dal punto di vista personale. Ciascuno deve decidere per sé quante informazioni desidera rivelare e per quali scopi. Se si desidera avere il pieno controllo sulla propria vita allora è opportuno pubblicare su Internet indirizzi, foto, interessi e anche opinioni solo con moderazione. In ogni caso non si dovrebbero caricare su Internet dati personali o effettuare operazioni in modo ingenuo. Inoltre, è opportuno studiare sempre attentamente le condizioni generali di contratto e le altre disposizioni in materia di protezione dei dati di ogni servizio online utilizzato.

Da considerare
La decisione che ciascuno prende è personale. Bisogna chiedersi: quanto conta per me la libertà e quanto invece il vantaggio di un servizio comodo e (quasi) gratuito? Vanno analizzate inoltre attentamente le informazioni con le quali si desidera poter essere confrontati magari anche cinque anni dopo.
Internet infatti non dimentica nulla. Spetta a ogni singolo individuo prendere la propria decisione.

2.3.3. Ricerca e falsificazione di profili

Le persone con cui si hanno rapporti di qualsiasi tipo, in particolare i datori di lavoro attuali e futuri, possono cercare persone su Google e analizzarne i profili sui social network.
Non tutte le informazioni disponibili su Internet su una determinata persona vanno a vantaggio di quest'ultima.
I profili possono anche essere falsificati con spiacevoli conseguenze per le persone interessate. Cercare il proprio nome mediante motori di ricerca specializzati nei social network come www.yasni.ch verificando i risultati, può aiutare a evitare questi malintesi. Va chiesto ai gestori dei siti Web contenenti dati errati di cancellare o correggere le pagine in questione.

2.3.4. Intenzioni criminali

I dati del titolare di un profilo possono finire nelle mani di persone con cattive intenzioni o addirittura con intenzioni criminali. Se i dati e le informazioni non vengono protetti adeguatamente o se non vengono gestiti con attenzione, ne possono risultare conseguenze indesiderate.

2.3.5. Phishing

Vengono definiti phishing i tentativi di malintenzionati di ottenere i dati di un utente di Internet (ad es. dati dei suoi profili), commettendo un furto di identità e danneggiando la persona in questione (ad es. accesso al conto bancario) con l'utilizzo, ad esempio, di indirizzi WWW falsificati, e-mail o messaggi brevi.

Il furto di dati su Internet allo scopo di utilizzare l'identità di qualcun altro può avere per la vittima gravi conseguenze, ad esempio a livello finanziario o di danno alla reputazione. Va quindi adottata la massima prudenza soprattutto nel campo dell'online banking, del commercio online e dei siti per single.

2.3.6. Shopping online

Nel campo dello shopping online ci sono molti pericoli e il phishing può diventare un problema proprio da questo punto di vista. Oggigiorno è possibile acquistare su Internet quasi tutto e le offerte a basso prezzo risvegliano l'interesse della clientela online. Affinché l'online shopping non diventi fonte di frustrazioni, a ogni acquisto è necessario verificare la serietà degli shop utilizzati. Va adottata la massima cautela soprattutto per gli acquisti all'estero. Se utilizzando siti ben noti in genere si evitano sorprese, per quelli sconosciuti è meglio leggere attentamente le condizioni generali di contratto. Anche il metodo di pagamento è un indizio della serietà del fornitore.

Consigli per salvarsi dalle truffe nell'ambito dello shopping e delle aste– nonaboccare.ch
https://www.nonabboccare.ch/it/truffa_e_furto_di_dati#!truffe_nell_ambito_dello_shopping_e_delle_aste_online

Dossier Truffe in Internet – skppsc.ch
https://www.skppsc.ch/it/temi/internet/internet-cybertruffa/?noredirect=it_IT

Acquisti su Internet
https://www.aranzulla.it/come-acquistare-su-internet-21416.html

Phishing – tentativi di frode sempre più raffinati
http://www.fastweb.it/web-e-digital/phishing-cos-e-e-come-difendersi/

Storie di Internet - Ufficio federale delle comunicazioni (UFCOM)
http://www.thewebsters.ch/it/

Attenzione alle truffe in Internet! (opuscolo) – Segreteria di Stato dell'economia (SECO)
https://www.seco.admin.ch/seco/it/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/vorsicht-vor-internetfallen-.html

2.4. Rischi concreti e conseguenze giuridiche

2.4.1. Cyberstalking

Si parla di cyberstalking quando le possibilità di contatto offerte dai social network vengono utilizzate dolosamente per esercitare pressione psicologica su qualcuno. Inoltre, la quantità di dati che gli utenti rivelano su di sé può far sì che qualcuno ne scopra l'indirizzo di domicilio, venga a conoscenza delle loro abitudini e li possa pertanto pedinare anche fisicamente.

Polizia della città di Zurigo, Schaugenau.ch – Cyberstalking (consigli e possibili contromisure)
https://www.nonabboccare.ch/it/molestie#!cyberstalking

2.4.2. Cybermobbing

Se una persona viene molestata, vessata o addirittura terrorizzata da altri via Internet per un lungo periodo – una situazione che tra i giovani si verifica abbastanza spesso – si parla anche di cybermobbing. La vittima viene molestata attraverso la pubblicazione su Internet di foto o video falsificati, imbarazzanti o schietti oppure di informazioni offensive. I malintenzionati possono tormentare e mettere in difficoltà le proprie vittime anche tramite profili falsificati di community online (ad es. Instagram, Facebook). Le vittime di tali attacchi ne soffrono molto.

Che cosa dice la legge sul cybermobbing?

- Se vengono pubblicati video o foto senza il consenso della persona interessata, sussiste una violazione della sfera privata e dei diritti sulla propria immagine.
- Chi offende o molesta costantemente altre persone tramite e-mail, Instant Messenger, SMS o altri canali può andare incontro a conseguenze penali.
- Se ad esempio vengono diffuse falsità o pronunciate offese tramite forum, social network o blog, è possibile far valere il proprio diritto alla cessazione o sporgere denuncia penal. Molestie, minacce, ricatti, diffamazioni e coercizioni sono reati, indipendentemente dal mezzo utilizzato e dal fatto che si tratti di un mezzo pubblico o chiuso. **Casi di questo genere devono essere denunciati alla polizia.**

2.4.3. Cyberbullismo

Questo termine definisce il tentativo di tiranneggiare delle persone attraverso la pubblicazione, ripetuta e intenzionale, su Internet di contenuti offensivi e/o umilianti, nonché con la minaccia di violenza. Il «bullismo» è appunto l'atto di tiranneggiare, tormentare o addirittura terrorizzare qualcuno.

We live security – Prevenire il cybermobbing
https://www.skppsc.ch/it/temi/internet/cybermobbing-cyberbullismo/?noredirect=it_IT

2.4.4. Sexting e sextortion

«Il sexting è la comunicazione privata su tematiche sessuali tramite mobile messaging. In senso stretto si tratta dell'utilizzo di linguaggio scurrile (in inglese «dirty talk)» per eccitarsi reciprocamente. Da quando esistono i Multimedia Messaging Services (MMS) e gli Instant Messenger come WhatsApp, è possibile anche l'invio di foto e video erotici del proprio corpo tramite applicazioni di Instant Messaging da terminali mobili.»
Definizione: Wikipedia https://it.wikipedia.org/wiki/Sexting

Sebbene la comunicazione privata, anche su tematiche sessuali, sia in linea di principio consentita dal diritto penale, esistono rischi correlati alla protezione dei dati e al diritto penale che è opportuno osservare.

- Chi diffonde foto o video di sé, commette un reato se si tratta di violenza sessuale o di atti con animali. Questo tipo di contenuti costituiscono pornografia illegale.
- Le rappresentazioni di sesso tra minori (sotto i 18 anni) o di minorenni in pose sexy sono considerate pedopornografia e comportano conseguenze penali. Inoltre i minorenni ne devono essere assolutamente informati.

- Sono considerate pedopornografia da un lato le rappresentazioni di atti sessuali con minori (sotto i 18 anni). Sono tuttavia vietate anche le rappresentazioni di minori anche nel caso in cui non vengano mostrati atti sessuali, cioè ad esempio di selfie con minori in pose chiaramente provocanti. È vietato produrre, guardare, possedere o inviare materiale pedopornografico. Il sexting può essere pedopornografia!

(Fonte in tedesco: https://www.lilli.ch/sexting_kinderpornografie/)

Website Pornografia illegale – skppsc.ch
https://www.skppsc.ch/it/temi/abusi-sessuali/pornografia-illegale/?noredirect=it_IT

Opuscolo Pornografie: Tutto ciò che prevede la legge – skppsc.ch
https://www.skppsc.ch/it/wp-content/uploads/sites/7/2016/12/leggepornografia.pdf

- Il principale rischio del sexting consiste nel fatto che i contenuti vengono diffusi molto rapidamente ed è molto difficile riuscire a cancellarli. Basta un singolo clic e una foto o un video compromettenti possono finire su Internet, dove resteranno probabilmente per sempre. Anche se le immagini vengono inviate consapevolmente – ad esempio a una persona degna di fiducia o sotto la pressione di un gruppo – possono causare gravi problemi se finiscono in mani sbagliate e/o vengono rese accessibili a un vasto pubblico.
- La «Sextortion» è una forma di ricatto correlato al sexting. Sotto falsa identità, un adulto si procura tramite i social network o tramite Internet immagini di giovani nudi, minacciando di pubblicarle per ottenere ulteriori immagini (ad es. uno striptease davanti a una Webcam accesa), denaro o un incontro con la vittima.

(Fonte: http://www.giovaniemedia.ch/it/opportunita-e-rischi/rischi/sexting.html)

Conclusioni
Come già accennato più volte, anche in questo caso vale il principio che: Internet non dimentica mai! È quindi necessario valutare bene se le foto o i video da inviare sono destinati a un vasto pubblico poiché la loro pubblicazione, voluta o non voluta, non può mai essere esclusa. I contenuti caricati una volta su Internet possono ricomparire in qualsiasi momento. In casi di questo tipo è possibile rivolgersi per consulenza e aiuto a Pro Juventute (chiamata o SMS a 147 oppure sul sito 147.ch), a un consultorio cantonale per le vittime oppure ad assistenti sociali scolastici, insegnanti e, naturalmente, ai propri genitori o altre persone di fiducia (familiari e ottimi amici). È importante che i casi di questo tipo vengano discussi e scoperti, in modo da poter adottare misure, rimuovere il materiale pubblicato da Internet ed evitare ulteriori attacchi.

Link all'elenco dei consultori cantonali per le vittime:
http://www.sodk.ch/fachbereiche/familie-und-gesellschaft/opferhilfe/wwwopferhilfe-schweizch/adresslisten/

2.5. Gli smartphone

Oggi uno smartphone dispone di innumerevoli programmi aggiuntivi. Alcune di queste applicazioni o «app» possono essere utilizzate inizialmente gratis, per poi ampliarne le

funzionalità o eliminare la pubblicità mediante un acquisto. Alcune app prevedono costi periodici di abbonamento. Le app raccolgono dati degli utenti che, di norma, non lo vengono a sapere e non hanno alcun controllo su tale processo. Vengono rilevati ad esempio dati come luogo, ora e frequenza di utilizzo dell'applicazione, ma anche gli SMS e i contatti salvati. Instagram e Facebook ad esempio si concedono un accesso completo ai dati presenti sul telefono, inclusi la posizione e gli SMS.

2.5.1. Geolocalizzazione – un vantaggio o un danno?

Con la geolocalizzazione, a un numero IP o a un altro indirizzo identificativo viene assegnata anche una posizione geografica. Un altro sistema per determinare la posizione di un utente è l'accesso tramite GPS o WLAN. Si tratta di una funzionalità che, se sui computer a volte è utile e risulta indispensabile per alcune app (ad es. quelle di navigazione), va invece giudicata in modo critico per quanto concerne la localizzazione degli smartphone.

Informare altri sul luogo in cui ci si trova oggi è di moda, ma nasconde anche dei pericoli. In tal modo comunichiamo ad esempio se ci troviamo a casa o siamo fuori, il che può interessare anche eventuali malfattori.

Anche da altri punti di vista vale la pena di chiedersi se sia opportuno che tutti siano sempre informati su dove si trova un utente in un determinato momento. Il rischio principale nell'utilizzo della funzione di geolocalizzazione di servizi online e app consiste nel fatto che la tecnica di localizzazione può essere utilizzata anche per creare profili degli spostamenti. Anche se tali profili non sempre possono essere attribuiti a una determinata persona, i dati raccolti su molti utenti di Internet e possessori di uno smartphone sono uno strumento interessante per ricerche di mercato e per l'industria valgono moltissimi soldi.

Google salva il profilo dei vostri spostamenti, ecco come cancellarlo
https://tecnologia.libero.it/difendere-la-privacy-modificando-le-impostazioni-di-google-1531

2.5.2. Diritto penale

Determinati contenuti sono in generale vietati e punibili penalmente: **contenuti lesivi dell'onore, razzisti, pedopornografici e nocivi per la gioventù.** Può essere punibile anche la pubblicazione su Internet di link a contenuti di questo tipo. Tali aspetti vanno considerati in caso di inoltro di contenuti «scabrosi», non solo su Internet ma anche ad esempio da cellulare a cellulare. Importante: la trasmissione di contenuti pornografici ai minori di 16 anni e proibito!

2.6. Videotelefonia

Esempi: Skype, FaceTime, Google Hangouts, Viber

Negli scorsi anni la videotelefonia ha assunto un ruolo sempre più importante nella comunicazione a livello mondiale. Sia per lavoro che privatamente, molte persone comunicano non più solo verbalmente, ma anche per iscritto e con il supporto della trasmissione audio e video. Diversi offerenti sono saliti su questo carro, dotando le proprie offerte per la comunicazione dell'opzione videotelefonia.

Per la scelta di messenger vanno però considerati diversi aspetti.

- I contenuti sono criptati durante la trasmissione?

- Sono al riparo dagli sguardi del fornitore del servizio tramite il salvataggio delle chiavi sui dispositivi degli utenti e non sui server?
- I vecchi messaggi possono eventualmente essere visualizzati a posteriori mentre sono protetti solo da chiavi di breve durata (password che scadono dopo un certo periodo di tempo)?

(Fonte in tedesco: http://www.zeit.de/digital/datenschutz/2014-11/messenger-sicher-vergleich-eff)

Oltre al fornitore del servizio anche l'interlocutore deve essere valutato in modo critico. Chattare con sconosciuti è rischioso perché sia le immagini che l'audio possono essere registrati senza che la persona interessata se ne accorga. Per questo dati sensibili, affermazioni personali e immagini compromettenti non devono essere inviati o mostrati in videochat.

Le chat anonime mettono a rischio la sfera privata
http://www.konsumer.it/nuovetecnologie2/557-pericolo-di-chat-le-insidie-nascoste-sotto-la-voglia-di-comunicare-.html

2.7. Immagini e diritti d'immagine

2.7.1. Dai, metto qualcosa online...? (i diritti sulla propria immagine)

Se si scattano foto o si registrano video con lo smartphone, il cellulare o un altro dispositivo e poi tale materiale viene caricato velocemente su Internet senza riflettere, è molto facile incappare in una violazione dei diritti di altri sulla propria immagine, qualora nelle immagini siano riconoscibili altre persone.

Indipendentemente da considerazioni legate al diritto d'autore, per quanto concerne le foto esistono i diritti sulla propria immagine. Ciò significa che le persone raffigurate possono di norma decidere se e in quale forma una determinata foto può essere scattata e pubblicata. Per questo motivo le foto possono essere pubblicate solo una volta ottenuto il consenso delle persone in esse ritratte.

Il consenso non è necessario solo se...

- ...le persone fotografate appaiono solo casualmente insieme a un paesaggio o altri luoghi.
- ...le persone presenti non sono in primo piano.
- ...le immagini mostrano personaggi della storia contemporanea (quindi anche persone famose).

Quindi attenzione durante party, concerti e serate in discoteca: non tutte le foto e non tutti i video possono essere messi online senza autorizzazione!

Inoltre, è sicuramente consigliabile avere un atteggiamento critico per quanto concerne la pubblicazione di foto di sé: «a caldo» capita infatti di autorizzare la pubblicazione di una foto magari un po' spinta su un portale di gossip o su un social network. Anche riguardo ai selfie va adottata cautela.

A proposito, solo chi li ha scattati ha il diritto di pubblicarli. Pubblicare una foto senza avere prima chiesto il consenso dell'autore non è permesso, indipendentemente dal fatto che la foto sia o meno già disponibile su Internet.

2.7.2. Fotografie di gruppi di persone

Anche le foto di gruppi di persone possono costituire una violazione dei diritti della personalità, nella misura in cui le persone in questione siano riconoscibili. La violazione dei diritti della personalità è considerata meno grave se nessun singolo individuo emerge dal gruppo e viene percepito come tale.

2.7.3. Fotografie scattate in luoghi pubblici

Se le foto vengono scattate in un luogo pubblico, tutte le persone presenti ne hanno la percezione e le persone ritratte sono solo «elementi di contorno» (ad es. i passanti vicino a un monumento), è sufficiente che la relativa foto venga cancellata su richiesta delle persone fotografate (subito sul posto oppure in un secondo momento) oppure che si rinunci a pubblicarla. Non è quindi necessario contattare e informare le persone in questione.

2.7.4. Il consenso legale

In tutti gli altri casi è necessario ottenere il consenso degli interessati. Il consenso è valido soltanto se volontario e preceduto da un'informazione adeguata. Se una persona interessata si oppone alla pubblicazione, occorre rispettarne la volontà.

Chi scatta e pubblica fotografie di singole persone deve procedere in modo diverso. In questo caso il consenso generale descritto sopra non è sufficiente. Gli interessati devono infatti avere la possibilità di visionare le immagini destinate alla pubblicazione e devono essere informati in merito al contesto della pubblicazione. Occorre inoltre considerare che nel caso della pubblicazione di immagini di minorenni si deve chiedere anche il consenso delle persone cui è affidata la loro educazione (cioè che esercitano la potestà genitoriale).

2.7.5. Possibili conseguenze in caso di pubblicazione senza motivo giustificativo

Le persone le cui foto sono state pubblicate senza consenso possono opporsi in qualsiasi momento alla pubblicazione, facendo valere i propri diritti, se necessario, mediante azione civile. Se il tribunale arriva alla conclusione che sussiste una violazione illegittima della personalità, poiché le foto sono state pubblicate senza consenso o un interesse pubblico o privato preponderante, può ordinare, oltre alla rimozione o distruzione delle foto in questione, anche il pagamento di un risarcimento danni e/o di una riparazione morale.

(Fonte: https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/pubblicazione-di-fotografie.html)

2.8. Altre tecnologie

2.8.1. Trasferimento dati su un cloud

Esempi: iCloud, One Drive, Dropbox

Il trasferimento di dati su un cosiddetto «cloud» (ingl. nuvola) ha per l'utente il vantaggio che non viene consumato spazio di memoria a livello locale sul PC, il laptop o lo smartphone perché i dati vengono salvati online. Molte app utilizzano automaticamente questa possibilità, caricando i contenuti dell'utilizzatore del telefono cellulare su un cloud, in parte anche senza che l'utente se ne accorga. Alcune applicazioni per la gestione delle foto (ad es. Google Fotos) salvano le immagini direttamente nel cloud subito dopo che vengono scattate, a meno che l'utente non abbia disattivato tale funzione.

Rischi connessi all'utilizzo di cloud

- **Perdita di controllo sui dati:** a causa della ramificazione internazionale delle reti e della virtualità, il luogo di conservazione dei dati spesso non è riconoscibile. Questo vale in particolare per i public cloud. L'utente del cloud non sa pertanto esattamente dove vengono salvati ed elaborati i suoi dati nel cloud. L'utente non sa nemmeno se vi sono subappaltatori coinvolti e se essi garantiscono un'adeguata protezione dei dati.

- **Accesso ai dati da parte di autorità straniere:** in molti casi per essere trattati nel cloud i dati vengono diffusi all'estero. Spesso i dati vengono salvati e trattati anche in Paesi che non dispongono di (sufficienti) norme sulla protezione dei dati. I fornitori di servizi di cloud computing sono però eventualmente tenuti a consentire ad autorità o tribunali stranieri l'accesso ai dati nel cloud; ciò anche se i dati non sono trattati o memorizzati nel Paese in cui ha sede l'autorità interessata.

Indipendentemente dal fatto che i dati siano trattati in un cloud, **occorre sempre mettere in conto i seguenti rischi**.

- **Perdita di dati:** a seguito di furti, cancellazioni, errori di sovrascrittura o altre operazioni di modifica è sempre possibile che i dati vadano persi.

- **Guasti al sistema e alla rete**, nonché l'indisponibilità delle risorse e dei servizi noleggiati possono avere come conseguenza la perdita di dati oppure l'accesso ai dati da parte di persone non autorizzate: la confidenzialità, la sicurezza e l'integrità dei dati non sono pertanto più garantite.

Conclusioni

L'utente del cloud deve considerare attentamente quali applicazioni e dati desidera mantenere presso di sé e quali invece è opportuno trasferire su un cloud.
(Fonte: https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/cloud-computing/spiegazioni-sul-cloud-computing.html)

2.9. «Internet delle cose»

Il termine Internet delle cose definisce la connessione di oggetti a Internet, affinché tali oggetti possano comunicare autonomamente tramite la rete e svolgere così diversi compiti per conto dell'utilizzatore. Il campo di applicazione va dalla fornitura di informazioni di carattere generale all'invio automatico di ordini, fino ad arrivare alle funzioni di avviso ed emergenza.

(Fonte in tedesco: http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v4.html)

Esempi: braccialetti per il fitness, elettrodomestici connessi (ad es. termostati, contatori dell'elettricità, smart TV, stampanti, giocattoli con microfono e/o fotocamera).

(Fonte: Pixabay / Pixabay)

Molti degli apparecchi elettronici e delle funzionalità che, per la loro interconnessione, vengono considerati parte dell'Internet delle cose, non servono nella vita quotidiana. Anche se, a un primo sguardo, sembrano semplificare la vita ed essere in grado addirittura di svolgere determinati compiti autonomamente, ancora una volta è necessario essere scettici.
Affinché la nostra vita non venga determinata da questi dispositivi, dobbiamo essere certi che non solo ci appartengano, ma anche che ci ubbidiscano. Non sempre è facile.
Se questi apparecchi sono collegati a Internet, spesso non sono sufficientemente protetti.
Alcune funzioni sono addirittura intenzionali: i televisori tracciano le emittenti rilevando cosa guardiamo e quando oppure addirittura ascoltano mediante altoparlanti che registrano i nostri colloqui in soggiorno.
Se desiderate acquistare un apparecchio connesso in rete, è opportuno che consideriate – prima ancora di valutare le funzionalità del prodotto e i modelli dei vari produttori – quanto segue.

1. L'apparecchio mi serve veramente o svolge le stesse funzioni di un altro apparecchio che ho già (o che posso noleggiare) ma semplicemente è più bello da vedere? Lo scopo principale dell'apparecchio è magari solo fare scena, sembrare cool o conformarsi?
2. Mi servono veramente le funzionalità basate sulla connessione in rete? Anche se ciò significa che un malintenzionato potrebbe controllare completamente l'apparecchio a distanza? Immaginatevi il peggio e procedete considerando che il malintenzionato è sicuramente più furbo di voi. Le funzionalità aggiuntive valgono il sovrapprezzo o il maggior rischio?
3. Se la funzionalità basata sulla connessione in rete non cessa di funzionare (il produttore sospende il proprio servizio basato su cloud) o deve essere disattivata (per questioni di sicurezza): potrò continuare a utilizzare l'apparecchio?

(Fonte in tedesco: http://www.pctipp.ch/tipps-tricks/kummerkasten/sicherheit/artikel/weg-vom-internet-der-unsicheren-dinge-87430/)

«Internet delle cose»
https://protezionedatipersonali.it/internet-of-things

Consigli per una corretta gestione dei dati

2.10. Principi fondamentali

Gestione diligente dei dati e delle informazioni:

- comunicare solo i dati strettamente necessari per lo scopo previsto
- nel caso di moduli (concorsi ecc.) e profili online utilizzare i dati personali con parsimonia, risparmiare dati!
- Se possibile non fornire l'indirizzo, il numero di telefono e l'età (soprattutto di bambini).

Rispetto: la regola d'oro (un principio fondamentale dell'etica pratica)

- «Trattare gli altri come vorremmo essere trattati noi stessi.»
- «Non fare agli altri ciò che non vorresti venisse fatto a te stesso.»

2.11. Consigli concreti

2.11.1. Consigli generali per la sicurezza

- Utilizzare **password sicure** – minimo 8 caratteri, combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali – e garantire che siano custodite in modo sicuro
- Utilizzare una password diversa per ogni servizio (esistono utili programmi per la gestione delle password perché non è possibile ricordarsi così tante password differenti)
- Configurare il browser Internet in modo sicuro, cioè con impostazioni atte a proteggere la sfera privata
- Cancellare periodicamente i cookie
- Cancellare la cronologia del browser, in particolare sui computer pubblici
- Utilizzare un software antivirus e aggiornarlo regolarmente
- Utilizzare software di aziende/da fonti affidabili (in particolare gli add-on) – massima cautela con i programmi gratuiti
- Utilizzare **software aggiornato** ed eseguire periodicamente l'upgrade
- Utilizzare tecniche di criptatura per la trasmissione dei dati (prestare attenzione al lucchetto verde nella barra dell'indirizzo, il quale segnala una connessione criptata)

2.11.2. Social network

Esempi: Facebook, Instagram, Google+, Youtube

- Ciascuno è personalmente responsabile della protezione della propria sfera privata!
- Fare attenzione a come ci si presenta in rete.
- Ricorda: tutto ciò che scriviamo, postiamo, linkiamo ecc. fornisce anche informazioni su di noi.

- Foto o video imbarazzanti e informazioni strettamente personali non devono assolutamente essere messi in rete. Tali dati rivelano aspetti molto personali, possono costare il posto di tirocinio oppure causare guai.
- Riflettere su ciò che l'appartenenza a un gruppo rivela su di noi
- Gestire i dati del profilo con attenzione: meglio tralasciare indirizzo, numero di telefono, indirizzo e-mail ecc.
- Impostare il profilo su «privato». I dati devono essere visibili solo agli amici.
- Verificare che gli amici online siano veramente dei buoni conoscenti prima di concedere loro libero accesso a foto e dati privati. Non si può mai sapere ciò che faranno delle informazioni.
- Postare contributi solo dopo averli verificati e ponderati con attenzione.
- Evitare di esprimere emozioni e prese di posizione (eccessivamente) negative. Spesso in un momento di rabbia si scrivono cose di cui poi ci si pente.
- Caricare foto, indirizzi e altri dati (anche tag sulle foto) di amici, conoscenti ecc. solo con il loro consenso
- In breve: scegliere bene le informazioni che si desidera diffondere.
- Verificare periodicamente le impostazioni relative alla privacy e, se necessario, modificarle.

2.11.3. Smartphone e WLAN

- Installare e gestire reti WLAN solo se criptate. Proteggere l'accesso con una password e comunicarla con prudenza Ancora meglio: creare reti per gli ospiti.
- Disattivare la WLAN quando non viene utilizzata. In tal modo si aumenta la sicurezza perché si evitano attacchi all'interfaccia radio e si risparmia la batteria
- Utilizzare hotspot pubblici e WLAN offerte da gestori solo con prudenza e scetticismo (evitare di usare l'e-banking e limitare al minimo i login in servizi via Internet come i social network)
- Se possibile, utilizzare inviare i dati sensibili e importanti solo in formato criptato.
- Attivare la geolocalizzazione tramite GPS solo in modo mirato, cioè in caso di effettiva necessità (in caso di richiesta di consenso all'attivazione riflettere se la geolocalizzazione è necessaria per un determinato servizio/una determinata app)
- Utilizzare solo app provenienti da fonti sicure (app store ufficiali)
- Prima di scaricare una app è opportuno informarsi tramite le descrizioni e valutazioni degli utenti e leggere le CGC e le disposizioni in materia di protezione dei dati.
- Utilizzare le importazioni per la sicurezza dei sistemi operativi: utilizzare il software operativo attuale installando immediatamente gli aggiornamenti.
- Limitare l'accesso delle app alle informazioni necessarie. È necessario che la app possa accedere a contatti, calendario, GPS e messaggi?

Smarrimento dello smartphone – Non si perde solo l'apparecchio, anche i dati personali sono in pericolo!

- Quantomeno l'accesso da parte di terzi può essere reso difficoltoso o addirittura impedito impostando preventivamente una password per l'accensione e lo sblocco.
- Alcune aziende offrono un software per la «cancellazione a distanza» dei dati dal proprio PC.
- Creare periodicamente un backup in formato criptato (a livello locale invece che sul cloud).

2.11.4. Supporti dati digitali

- Disattivare la funzione Autorun delle chiavette USB connesse al computer.
- Verificare regolarmente che il supporto dati non contenga virus.
- Utilizzare esclusivamente supporti dati provenienti da fonti sicure e da persone di cui ci si può fidare.

Smarrimento della chiavetta USB o del disco rigido portatile - i dati sono a rischio!

- Criptare i dati personali sensibili e riservati sui supporti dati digitali!

2.11.5. Chat

- Scegliere chat con un moderatore che controlla quanto accade.
- Pensare a un buon nickname (nomi di fantasia, parole divertenti, un nome che non susciti strane associazioni); non utilizzare il proprio vero nome e non indicare l'età, il luogo di domicilio o la scuola.
- Indirizzo, numero di telefono e cognome non devono mai essere rivelati.
- Avere un atteggiamento rispettoso e utilizzare un tono adatto: vale la «Chatiquette» (vedi sotto).
- Cautela negli incontri di persona con gente conosciuta in chat (informare i genitori).
- Una sana dose di diffidenza è utile. Non fornire troppe informazioni personali.
- Non inviare direttamente messaggi riservati a sconosciuti.

Se accade qualcosa che appare strano

- Reagire immediatamente e informare qualcuno! Possono fornire aiuto i genitori, una persona di fiducia o gli insegnanti.
- Interrompere immediatamente il dialogo

Come essere un buon cittadino della rete http://faqintosh.com/netiquette.html

2.11.6. Forum e blog

Esempi: Twitter (Mikroblogs), Blogger (Google), forum sul Web (innumerevoli)

Netiquette

La prima fondamentale raccomandazione della nostra Netiquette di Usenet è:
«Non dimenticare mai che dall'altra parte c'è una persona!»
(Fonte in tedesco: http://www.usenet-abc.de/wiki/Team/Netiquette)

Regole generali della Netiquette

- Non offendere, la cortesia ha la precedenza
- Essere il più concisi possibile
- Evitare affermazioni ironiche
- Scrivere in modo corretto (incl. le maiuscole e minuscole)
- Citare correttamente (incl. le virgolette, se necessario e se possibile indicando la fonte)
- Postare contributi solo dopo averli verificati bene

2.11.7. Moduli online di aziende, fornitori di servizi e autorità

- Principio fondamentale: inviare dati personali solo a contatti affidabili e solo se serve a ottenere un vantaggio.
- Leggere con attenzione le Condizioni generali di contratto (CGC), in particolare il capitolo dedicato alla protezione dei dati. Vi si trovano indicazioni su quali dati personali vengono salvati, inoltrati a terzi o utilizzati per scopi pubblicitari. Poi valutare bene se si intende veramente utilizzare una app alle condizioni indicate.
- Per tutti i servizi di pagamento (carte di credito, Paypal) va adottata particolare cautela: siate scettici!
- Non fornire mai a terzi dati dell'account, numeri di carte di credito o password. Le banche non contattano i propri clienti per e-mail e non chiedono la password o il nome utente.
- Se si riceve un'e-mail sospetta non aprire gli allegati o eventuali link.
- Ottenere informazioni sul fornitore del servizio e sulla sua serietà.
- Verificare ciò che è possibile fare in caso di tentativi di phishing.

Qual è il comportamento corretto in caso di phishing?
https://www.skppsc.ch/it/temi/internet/phishing/?noredirect=it_IT
https://www.melani.admin.ch/melani/it/home/themen/phishing.html
http://www.techeconomy.it/2015/08/20/come-riconoscere-difendersi-dal-phishing/

2.11.8. Instant Messenger e telefonia via Internet

Esempi: Skype, WhatsApp, Snapchat ecc.

Consigli generali per la sicurezza

- Scegliere un messenger che consenta di effettuare impostazioni per la sicurezza.
- Impostare il messenger in modo che i nuovi contatti debbano essere accettati prima che vengano inseriti nella lista dei contatti.
- Non fornire superficialmente a sconosciuti il proprio nome utente nel messenger
- Inserire nella lista dei contatti solo buoni amici e consentire solo a tali persone di inserire il nostro nome nella loro lista dei contatti (in alcuni messenger l'inserimento non può più essere annullato)
- Cancellare i contatti indesiderati, maleducati e invadenti oppure bloccarli con la funzione «Ignora».
- Leggere solo messaggi e prendere solo chiamate di persone presenti nella propria lista dei contatti.
- Disattivare l'indicazione pubblica dello status.
- Salvare automaticamente la cronologia dei messaggi.
- Disattivare l'immagine visualizzata e la trasmissione via Webcam.
- In linea di principio, non aprire file o link inviati da sconosciuti, i quali possono contenere virus, trojan ecc. Come per la trasmissione video o telefonica, si tratta di una funzione che purtroppo non tutti i messenger consentono di bloccare.
- Non cliccare mai su un link ricevuto nella finestra dei messaggi senza essersi prima accertati che la persona in questione lo abbia davvero inviato volontariamente. Per i worm contenuti nelle e-mail, anche altri programmi dannosi possono inviarsi automaticamente a tutte le persone contenute nelle liste dei contatti. Anche se i link provengono da persone conosciute, possono quindi comunque comportare dei rischi dei quali il mittente non è al corrente.

2.12. Dati di altri: bisogna essere corretti!

- La personalità degli altri va rispettata!
- Non mettere in rete foto, video o informazioni (ad es. nome utente, numeri, indirizzi, password ecc.) di altri senza il loro consenso!
- Fare attenzione ai **dati sensibili**!
- Va evitato assolutamente di diffondere novità sugli altri che le persone interessate non vogliano diffondere o non abbiano ancora diffuso personalmente.
- È vietato pubblicare informazioni errate o diffamanti su qualcuno. La diffamazione è un reato punibile!

Rispettare il diritto penale

- Non è consentito inoltrare e diffondere contenuti lesivi dell'onore, sediziosi, (pedo)pornografici e nocivi per la gioventù.
- In caso di dubbio la regola è: lasciar perdere e informare la persona di fiducia!

Codice penale svizzero (CPS):

tra l'altro. art. 19714. Pornografia

4. Pornografia

Chiunque offre, mostra, lascia o rende accessibili a una persona minore di sedici anni, scritti, registrazioni sonore o visive, immagini o altri oggetti o rappresentazioni pornografici, o li diffonde per mezzo della radio o della televisione, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

(Fonte: https://www.admin.ch/opc/it/classified-compilation/19370083/index.html)

Restare se stessi!

Internet è solo apparentemente uno spazio anonimo e non vi è assolutamente alcun vuoto giuridico.
Non bisogna quindi fare nulla che non si farebbe anche nella vita reale.
Si tratta di evitare tutto ciò di cui ci si potrebbe successivamente pentire.
Bisogna restare corretti e restare se stessi. Anche in rete!

3. Glossario

3.1. Termini relativi alla protezione dei dati

Cittadino/uomo trasparente	La radiografia completa di un individuo e del suo comportamento. Riferimento alla protezione dei dati: rivelando informazioni personali rischiamo di perdere la nostra sfera privata.
Diritto all'autodeterminazione informativa	Ogni persona deve poter decidere autonomamente quali informazioni sul proprio conto vengono rese note, quanto, dove e a chi, nonché per quale scopo vengono utilizzate.
Dati riferiti alla persona (o dati personali)	Dati su una persona determinata o determinabile. Basta quindi che dai dati sia possibile risalire alla persona cui appartengono. Non è necessario che venga citato un nome.
Dati degni di particolare protezione	Informazioni e dati particolarmente sensibili per i quali va adottata particolare cautela. Ne fanno parte ad esempio le attività di carattere religioso o politico, le informazioni relative alla sfera intima e i dati sulla salute.
Sfera privata	Spazio non pubblico nel quale un essere umano può esercitare indisturbato il proprio diritto alla libera evoluzione della personalità al riparo da influssi esterni.
Sfera intima	Ambito concernente i pensieri e i sentimenti più intimi di un essere umano; ambito delle esperienze delle quali una persona in genere non parla volentieri e che essa protegge accuratamente dall'ambiente circostante per ragioni di tatto o di preservazione dell'amor proprio (ad es. sessualità).

3.2. Definizioni tratte dalla legge federale sulla protezione dei dati

Trattamento	Qualsiasi operazione relativa a dati, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione o la distruzione di dati.
Comunicazione	Il fatto di rendere accessibili i dati, ad esempio l'autorizzazione della consultazione, la trasmissione o la diffusione.
Persone interessate	Persone fisiche o giuridiche i cui dati sono oggetto di trattamento.
Collezione/raccolta di dati	Ogni complesso di dati personali la cui struttura permette di ricercare i dati secondo le persone interessate.
Detentore di una collezione di dati	La persona privata o l'organo federale che decide in merito allo scopo e al contenuto della collezione di dati.

3.3. Termini relativi a Internet

Banner	Spazio pubblicitario (su Internet con link a un dominio/un sito Web).
Browser	Software, che permette di visualizzare i contenuti del WWW. Programma per computer per accedere a Internet (ad es. Internet Explorer, Google Chrome, Firefox).
Chat	Possibilità di comunicare in tempo reale tra diversi utenti mediante Internet; comunicazione online che si effettua tramite la tastiera. L'utente può scegliere tra diverse «Chatroom» e anche decidere con chi (non) desidera «parlare».
Cookie	File di testo che vengono generati sul computer dell'utente quando si visualizzano pagine Internet. In questi file vengono salvate informazioni sull'utilizzo di Internet da parte dell'utente. I cookie possono essere oggetto di interrogazioni dall'esterno. Le impostazioni del browser permettono però di bloccarli.
Domain	Alias alfanumerico per numeri/indirizzi IP. I domini possono essere suddivisi secondo criteri tematici o geografici. *Esempi:* *.com = sito commerciale* *.ch = sito svizzero o dominio registrato in Svizzera* *.org = dominio originariamente non commerciale* *.edu = scuole e università*
Firewall	Componente che separa una rete da Internet. Serve a proteggere da virus e accessi non autorizzati alla propria rete.
FTP	File Transfer Protocol; consente lo scambio di file tra due computer collegati a Internet (se entrambi hanno il protocollo FTP attivato). In tal modo è possibile copiare dati su un computer collegato a Internet o scaricarli da tale computer.
Hacker	Persona che si procura un accesso non autorizzato a sistemi informatici di terzi.
http	L'Hypertext Transfer Protocol (http) è un protocollo per il trasferimento di dati tramite una rete. Viene utilizzato principalmente per caricare in un browser siti Web presenti sul World Wide Web (WWW).
https	Anche SSL HTTPS; un metodo per la trasmissione di dati in formato criptato. I dati vengono criptati mediante SSL e trasmessi tramite http.
Indirizzo IP	Una specie di «numero di telefono» per una sessione di navigazione in Internet. Si compone di quattro blocchi di numeri compresi tra 0 e 255 e separati da un punto. *Esempio 62.2.169.0*

Malware	Software maligno – Programmi dannosi (a volte utilizzato come sinonimo di virus) che vengono installati involontariamente dall'utente o senza che quest'ultimo se ne accorga e che danneggiano il computer.
Newsgroup	Forum di discussione su Internet
Social Media	Vedi Web 2.0
SNS	Social Network Services – Gestori di social network *Esempio: Facebook*
SSL	Tecnica di criptatura per Internet
Provider	Fornitore di servizi Internet *Esempi: upc, swisscom, sunrise*
URL	Uniform Ressource Locator. Un sistema che consente di raggiungere un sito su Internet. Può essere definito anche «l'indirizzo» di un sito Web. *Esempio: www.sbb.ch*
***Web* 2.0**	Applicazione interattiva su Internet. L'utente non è solo consumatore ma diventa soggetto attivo fornendo e caricando informazioni e dati.
WLAN	Wireless Local Area Network – rete senza fili

4. Fonti, link e rinvii

Tema/Parole chiave	Link
Incaricato federale della protezione dei dati	https://www.edoeb.admin.ch/edoeb/it/home.html
Protezione dei dati su Internet	https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer.html
Consigli e informazioni su Internet	http://www.giovaniemedia.ch/it/home.html http://www.klicksafe.de/
Sicurezza su Internet	https://www.skppsc.ch/it/ https://www.nonabboccare.ch/it/home
Violenza e pericoli su Internet	http://www.giovaniemedia.ch/it/opportunita-e-rischi/rischi/violenza.html http://www.netcity.org/
Social network	http://www.giovaniemedia.ch/it/opportunita-e-rischi/media-sociali.html
WLAN	https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/wlan.html
Cloud Computing	https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/cloud-computing/spiegazioni-sul-cloud-computing.html
Telefono cellulare	https://www.nostrofiglio.it/bambino/quando-dare-cellulare-bambino
Raccolta di link (giovani/Internet)	https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/giovani-e-internet/link-sul-tema.html
Informazioni per i genitori	https://consulenza-per-genitori.projuventute.ch/index.php?id=2525&L=2

5. Elenco di referenti per vari tipi di problemi

5.1. Protezione dei dati

Incaricato federale della protezione dei dati e della trasparenza
Modulo di contatto:
https://www.edoeb.admin.ch/edoeb/it/home/l-ifpdt/contatto/formulario-di-contatto.html
oppure Tel. +41 (0)58 462 43 95

5.2. Per genitori e insegnanti

Elternnotruf: 0848 354 555 o elternnotruf.ch (in tedesco e francese)

Panoramica dei consultori regionali
http://www.giovaniemedia.ch/it/offerte-e-consigli/servizi-di-consulenza.html

LCH – Associazione mantello degli insegnanti in Svizzera (in tedesco)
https://www.lch.ch/publikationen/bildung-schweiz/

5.3. Per bambini e giovani

Consulenza e aiuto di Pro Juventute:
telefono e SMS 147, Informazioni e FAQ sul sito 147.ch/it

Siti Web per i giovani (informazioni, FAQ, forum) – in tedesco:
feel-ok.ch, tschau.ch, cybersmart.ch, frageinfach.ch, lilli.ch e drgay.ch

Elenco d'indirizzi dei consultori cantonali per bambini e giovani vittime di reati:
Adressen der kantonalen Opferhilfe-Beratungsstellen (OHG) für Kinder und Jugendliche:
http://www.sodk.ch/fileadmin/user_upload/Fachbereiche/Opferhilfe/Adresslisten/2018.06.06_OH-Beratungsstellen_Kinder_und_Jugend.pdf

Netla - Kampagne des Rats für Persönlichkeitsschutz
http://www.netla.ch/it

6. Articoli online e dossier

N.	Tema/Parole chiave	Link
1	Protezione dei dati, Internet, futuro	http://ricerca.repubblica.it/repubblica/archivio/repubblica/2018/05/30/proteggere-i-dati-personali-finalmente-la-direttiva-madre38.html?ref=search
2	Protezione dei dati, Internet, e-mail	https://www.swissid.ch/it/protezione-dei-dati
3	Protezione dei dati, Software, riconoscimento facciale	https://www.aranzulla.it/riconoscimento-facciale-foto-7425.html
4	Protezione dei dati, Internet, bambini, comportamento	https://www.educa.ch/it/guides/sicurezza-social-network/comportamento-internet-prevenzione
5	Internet, bambini e giovani, comportamento	http://www.educa.ch/it/guides
6	Dossier Facebook	https://www.tio.ch/cerca/facebook
7	Facebook, protezione dei dati	http://www.repubblica.it/tecnologia/sicurezza/2018/05/30/news/ceo_snapchat_attacca_facebook_poteva_copiarci_anche_la_privacy-197756678/?ref=search
8	Facebook, protezione dei dati, legge	http://www.repubblica.it/tecnologia/social-network/2018/04/20/news/facebook_nuove_regole_per_la_privacy_ma_varranno_solo_per_utenti_europei-194371678/
9	Facebook, numeri di telefono	https://tecnologia.libero.it/come-trovare-profili-facebook-utilizzando-numeri-di-telefono-9005
10	Facebook, sfera privata	https://www.laregione.ch/culture/societa/1262753/facebook--nuovo-scandalo-dati-personali-
11	Facebook, falsi amici	https://www.corriere.it/tecnologia/social/13_dicembre_04/chi-ci-odia-facebook-l-app-scopre-falsi-amici-31684180-5cd6-11e3-a319-5493e7b80f59.shtml
12	Facebook, dati propri	https://tg24.sky.it/mondo/2018/06/04/facebook-dati-utenti.html
13	Cloud Computing	http://www.kiteblue.it/cose-il-cloud/#
14	Caricamento video su Youtube: da denuncia?	https://blog.ehiweb.it/2017/04/10/youtube-copyright-video-diritti-autore/
15	Smartphone, app, dati personali	http://www.ingegneri.info/news/innovazione-e-tecnologia/app-privacy-smartphone-gdpr/
16	Phishing	https://www.melani.admin.ch/melani/it/home/themen/phishing.html